TISS CYBERSECURITY INSIGHTS

TRILLIUM INFORMATION SECURITY SYSTEMS

PEN TEST INSIGHTS REPORT 2024

TABLE OF CONTENTS

INTRODUCTION

In today's rapidly evolving digital landscape, cybersecurity is a critical priority for businesses across all industries. As technology advances, so do cyber threats—becoming more sophisticated, persistent, and damaging. Organizations must proactively identify and address security vulnerabilities before they can be exploited. Penetration testing plays a pivotal role in this process by assessing security controls, uncovering weaknesses, and ensuring compliance with global industry standards.

In 2024, Trillium Information Security Systems (TISS) conducted penetration testing engagements across key sectors, including banking, healthcare, government, IT services, finance, and telecommunications. These assessments spanned a broad spectrum of digital environments, testing web applications, mobile apps, networks, Active Directory environments, databases, servers, and cloud infrastructures.

The findings reveal a concerning reality—many organizations continue to struggle with fundamental security flaws. Weak access controls, outdated systems, and misconfigurations remain persistent issues, creating significant attack vectors for cybercriminals. While industries handling sensitive financial and personal data have made progress in security maturity, gaps in threat detection and remediation still expose them to evolving risks.

This report goes beyond listing vulnerabilities; it provides a data-driven analysis of security trends, common weaknesses, and sector-specific risks. By breaking down the types of assets tested and highlighting the vulnerabilities discovered, businesses can gain actionable insights to fortify their defenses.

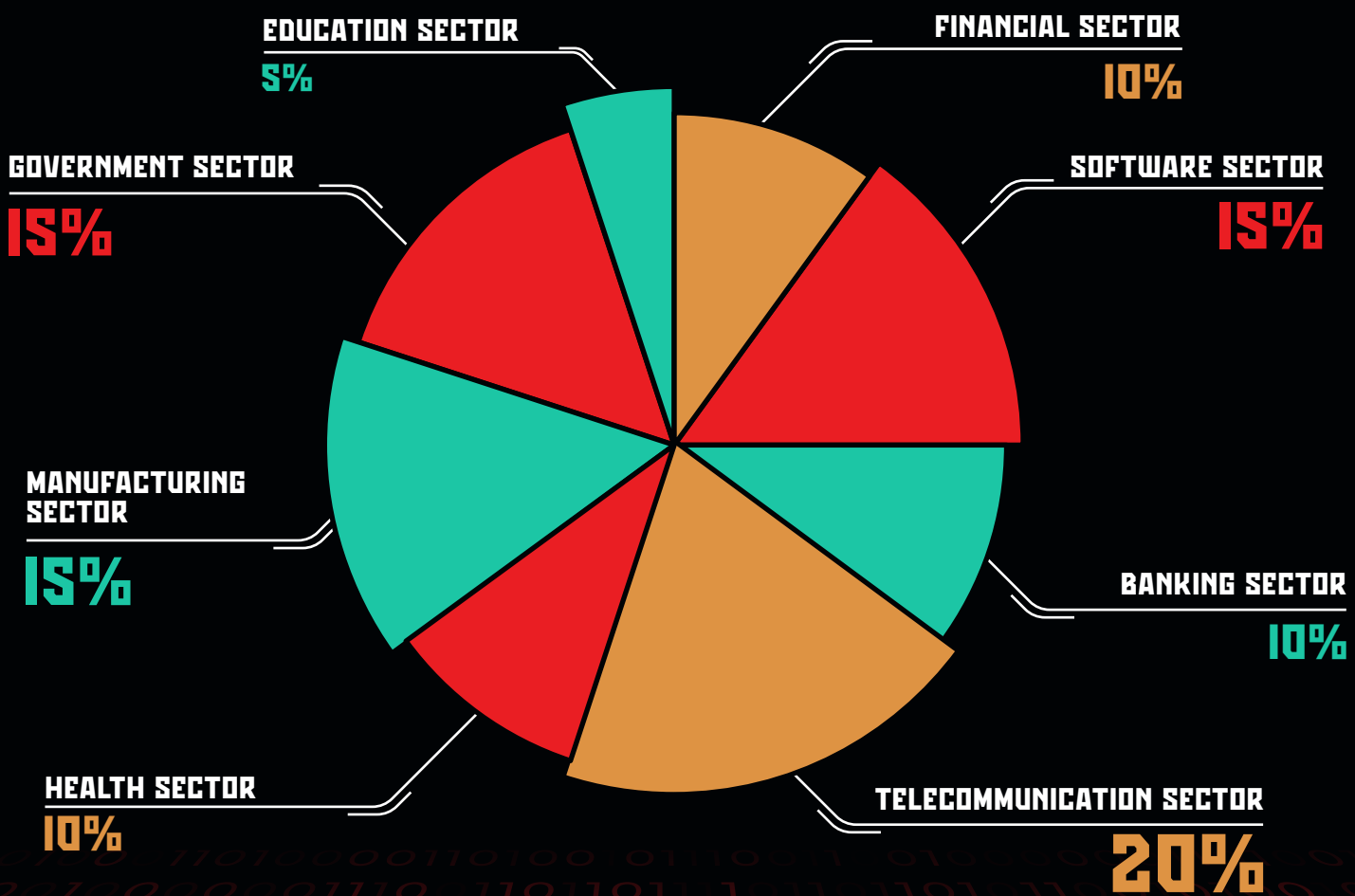
Cyber threats will only continue to evolve in complexity, making reactive security measures insufficient. Organizations must adopt continuous security testing, enforce strict patch management, and foster a strong cybersecurity culture to mitigate risks effectively. The insights from this report serve as a roadmap for businesses striving to strengthen their security posture, protect critical assets, and build long-term resilience against cyber threats.

ENGAGEMENT DEMOGRAPHIC

This report examines penetration testing engagements across multiple industries, evaluating the security of information systems, networks, and digital assets. These engagements covered critical sectors such as banking, government, education, and telecommunications, each facing unique cybersecurity challenges.

Telecommunications emerged as the most frequently assessed sector, accounting for approximately 20% of total engagements. This reflects the industry's increasing focus on securing large-scale digital infrastructures that are prime targets for cyberattacks. The software sector followed closely, also representing 20% of engagements—an indication of the growing security awareness among technology-driven organizations that manage intellectual property and customer data.

Cloud security remains a significantly under-tested area, with AWS Cloud instances representing only 0.22% of engagements. This may be attributed to the slower adoption of cloud infrastructure in Pakistan. The data highlights the distribution of security assessments across various sectors, showcasing the breadth of our testing coverage and the frequency of engagements in different industries.

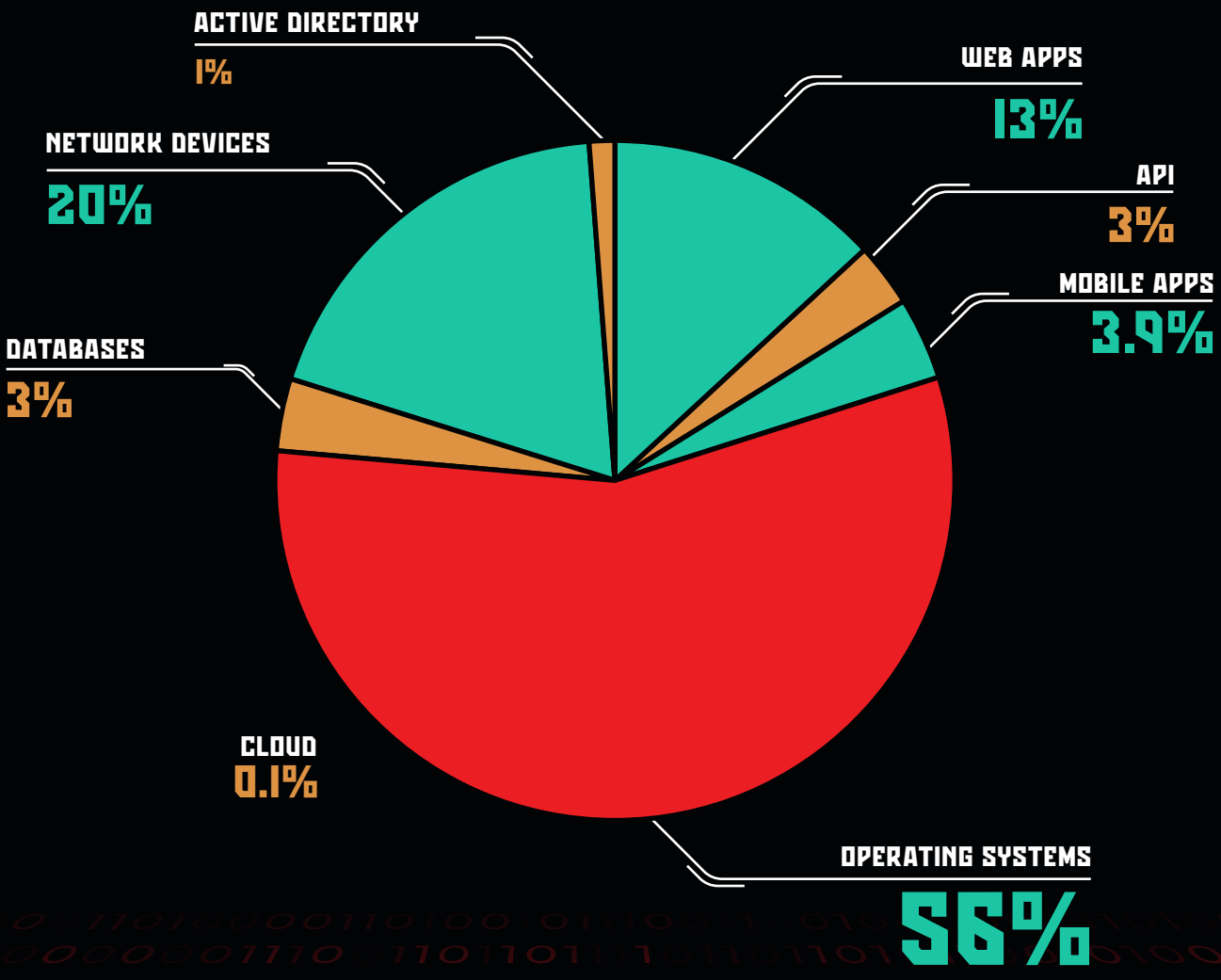


ENGAGEMENT FOCUS AREAS

Every penetration testing engagement involves evaluating multiple components of an organization's infrastructure, from endpoint devices to cloud environments. The most frequently tested assets included workstations, network devices, servers, and virtual machines, collectively making up 76% of all assessments. Web applications followed at 13%, reflecting their critical role in digital operations.

Security evaluations of databases, APIs, and mobile applications were notably lower, representing 3% and 4% of engagements, respectively. Cloud security assessments, though not entirely absent, remained the least prioritized, accounting for less than 1% of total tests. This could indicate a gap in cloud security testing or reflect the relatively slower adoption of cloud infrastructure in Pakistan compared to global trends. As cloud adoption grows, ensuring adequate security assessments will be crucial to addressing emerging cloud-specific threats and maintaining comprehensive security coverage.

ENGAGEMENT SCOPE

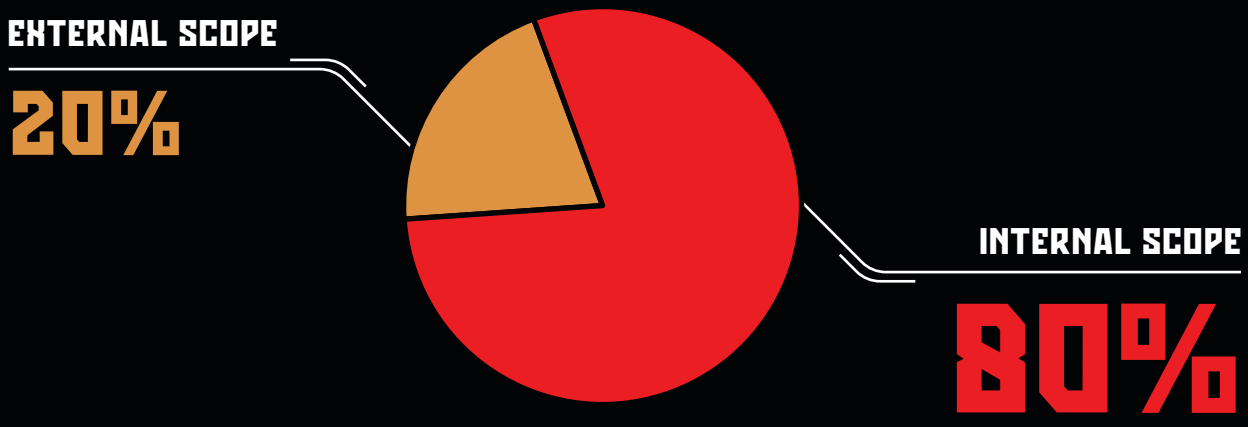


VULNERABILITIES IDENTIFIED

Our engagements assessed both external & internal perimeters, identifying vulnerabilities that could be exploited by threat actors. External assessments simulated threat actors attempting to breach the network perimeter without prior access, while internal assessments focused on uncovering weaknesses within an organization's infrastructure that could lead to privilege escalation or data compromise.

Results showed that the 80% of vulnerabilities exist within internal environments, often due to misconfigurations, weak access controls, and outdated systems. While external assessments exposed critical security gaps, they frequently served as entry points to deeper internal network access. In many cases, testers successfully pivoted from external networks into internal environments, demonstrating how attackers could move laterally once inside.

Similarly, internal assessments often resulted in access to sensitive data or critical infrastructure, highlighting the risk posed by inadequate segmentation and privilege management. While not every test aimed to gain domain or enterprise administrative control, many engagements demonstrated that attackers could achieve privileged access with minimal effort.



VULNERABILITY TRENDS ACROSS ASSET TYPES

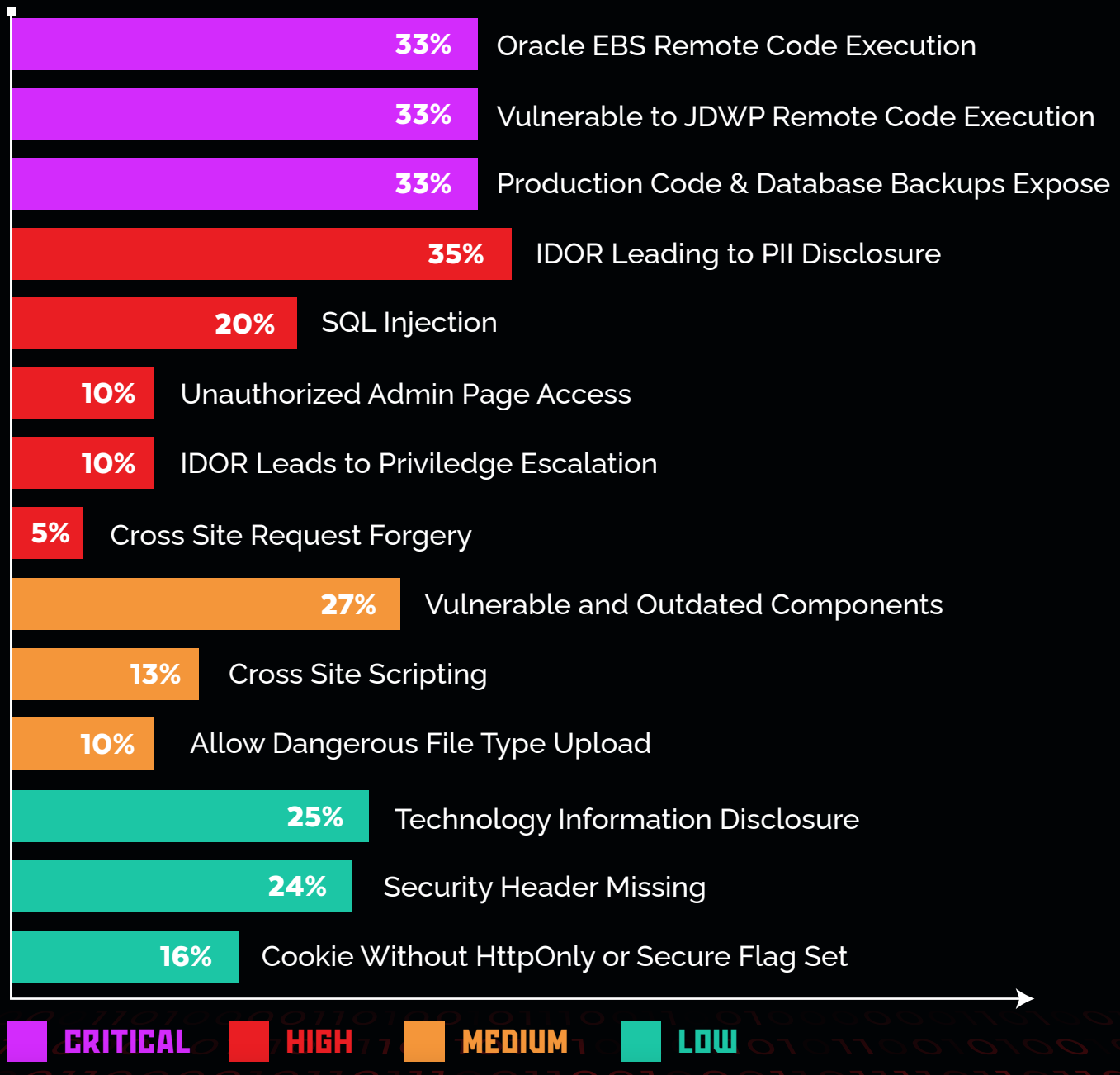
This section provides an overview of the most common security weaknesses identified across different asset types, categorized by severity levels: Critical, High, Medium, and Low. The following subsections will highlight key vulnerabilities found in network devices, servers, workstations, and web applications, along with their security implications.

Our assessments revealed recurring security flaws that could be exploited by attackers to escalate privileges and gain unauthorized access. Common issues included misconfigurations, outdated software, and weak authentication mechanisms. Web applications frequently suffered from injection attacks, mismanaged access controls, and insecure APIs, while network and endpoint security flaws were often linked to unpatched systems, weak credential policies, and poor segmentation.

WEB APPLICATIONS

Our assessment of web applications revealed several critical vulnerabilities, including Remote Code Execution (RCE) and exposed production code or database backups, which pose significant security risks. High-severity flaws such as Insecure Direct Object References (IDOR), SQL Injection, and Unauthorized Admin Access were frequently identified, increasing the risk of data breaches. Privilege escalation vulnerabilities further amplified these risks by allowing attackers to gain higher-level access and move laterally within networks.

Additionally, outdated components, missing security headers, and Clickjacking highlighted weaknesses in secure development practices, expanding the attack surface. To mitigate these risks, organizations should enforce robust access controls, conduct regular security assessments, and apply timely patches. Strengthening authentication mechanisms and ensuring proper security configurations can further reduce potential attack vectors.



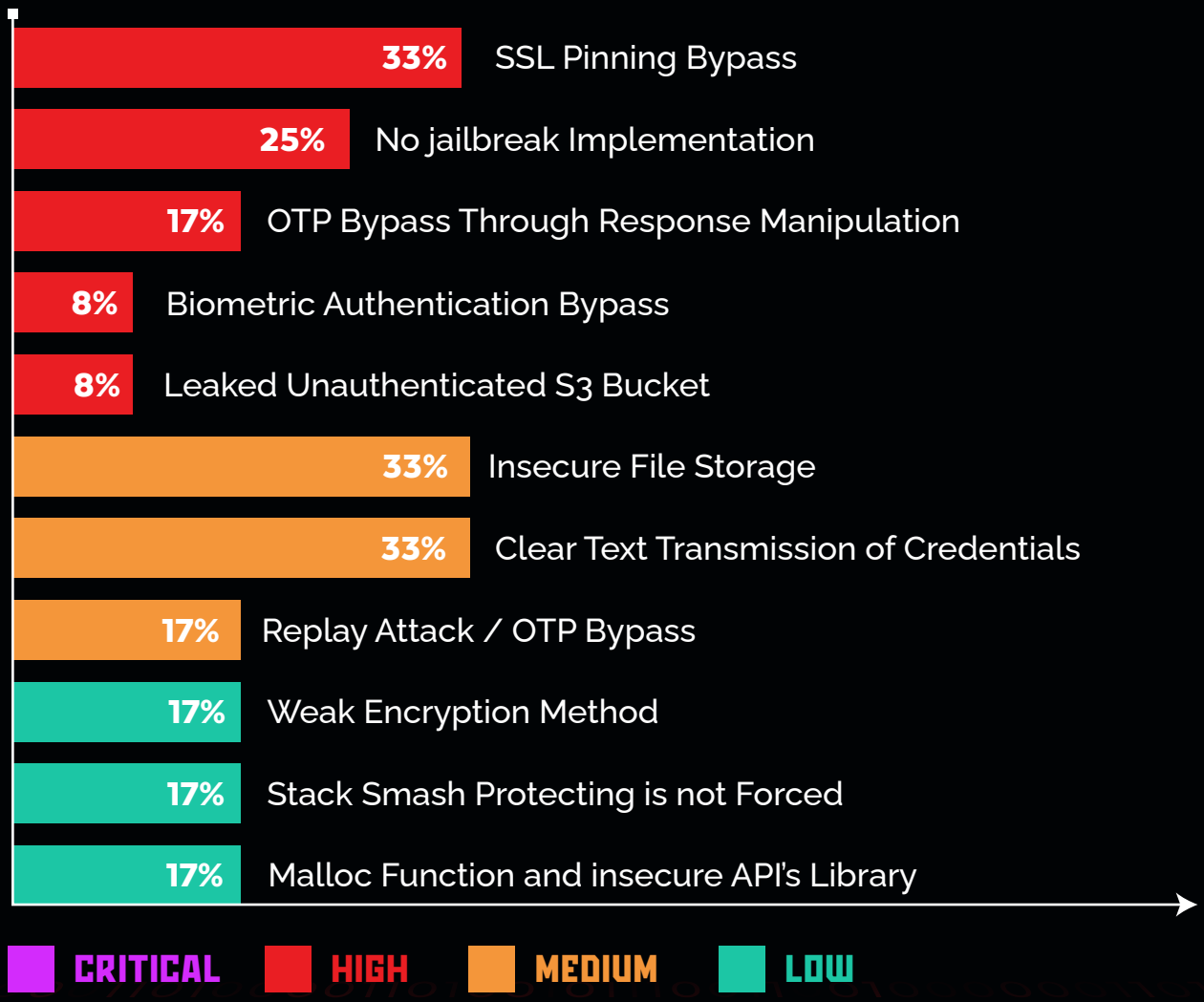
*Disclaimer: The graph displays the top critical & high, medium & low vulnerabilities.

MOBILE APPLICATIONS

Our assessments of mobile applications did not reveal any critical vulnerabilities, which may indicate improvements in mobile app security. However, several high-risk gaps, such as SSL Pinning Bypass, OTP Bypass, and the absence of Root/Jailbreak Detection, remain exploitable, potentially exposing sensitive data. Biometric Authentication Bypass and Insecure Transport also weakened security by increasing the risk of credential interception.

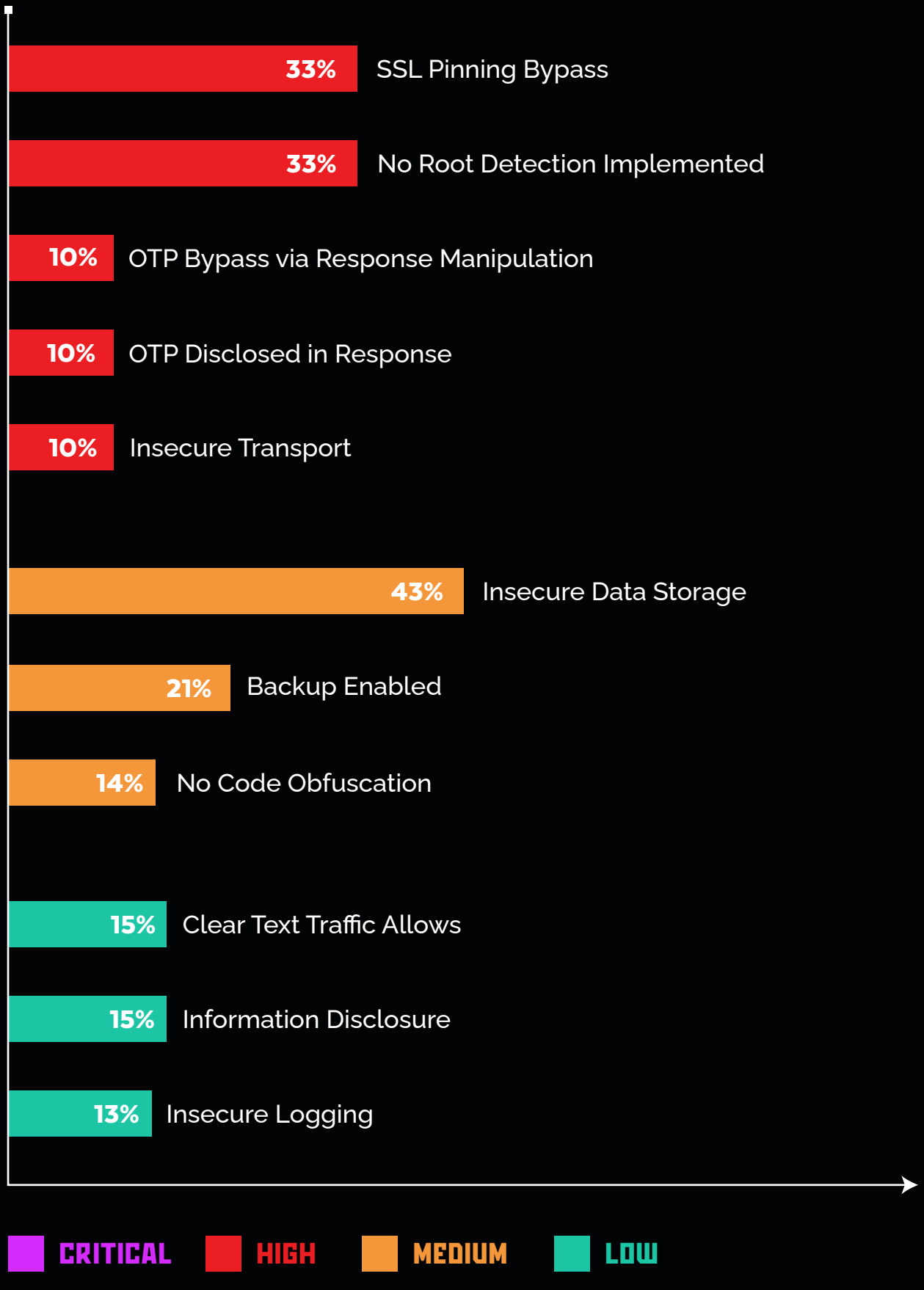
This year, we repeatedly identified medium-risk issues like Insecure Data Storage, Cleartext Transmission, and Lack of Code Obfuscation, which elevate the risk of data leaks and reverse engineering attacks. Additionally, low-risk vulnerabilities such as Weak Encryption and Insecure Logging highlighted gaps in secure coding practices. Strengthening encryption, enforcing stricter authentication controls, and improving secure storage mechanisms are essential steps to fortify mobile applications against evolving threats.

IOS APPLICATION



*Disclaimer: The graph displays the top critical & high, medium & low vulnerabilities.

ANDROID APPLICATION

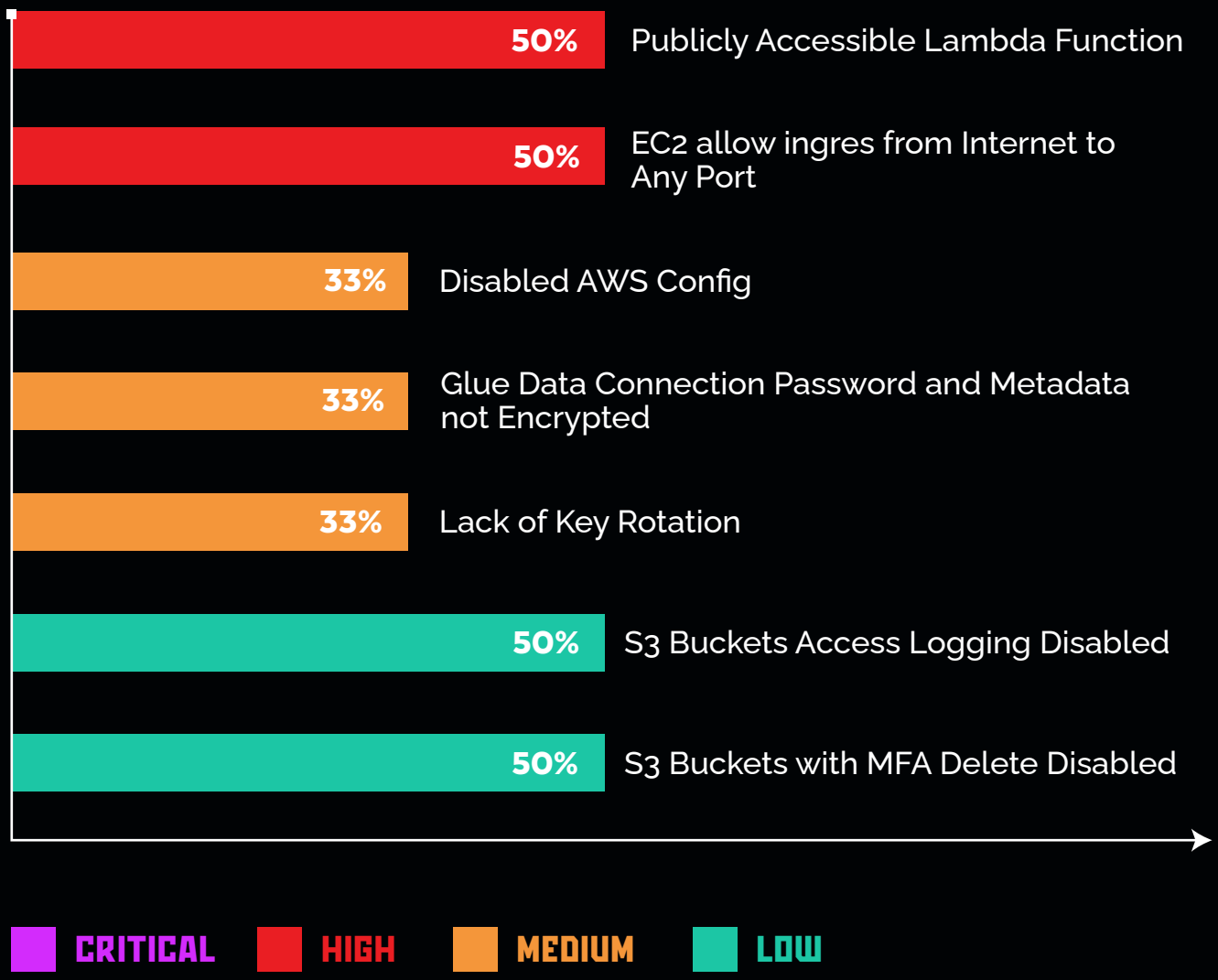


*Disclaimer: The graph displays the top critical & high, medium & low vulnerabilities.

CLOUD

While our assessments did not uncover any critical vulnerabilities but they revealed high-risk exposures that could leave systems vulnerable to attacks. Publicly accessible Lambda functions and EC2 instances allowing ingress from any port were among the most concerning issues, increasing the risk of unauthorized access and potential data breaches.

A recurring pattern was the presence of medium-risk misconfigurations, such as disabled AWS Config, unencrypted Glue Data Connection passwords, and lack of key rotation, which weaken security monitoring and access controls. Additionally, low-risk concerns like S3 buckets with disabled access logging and missing MFA Delete settings highlighted areas where data protection could be strengthened. Addressing these gaps through stricter access policies, encryption, and continuous monitoring is critical for securing cloud environments.



*Disclaimer: The graph displays the top critical & high, medium & low vulnerabilities.

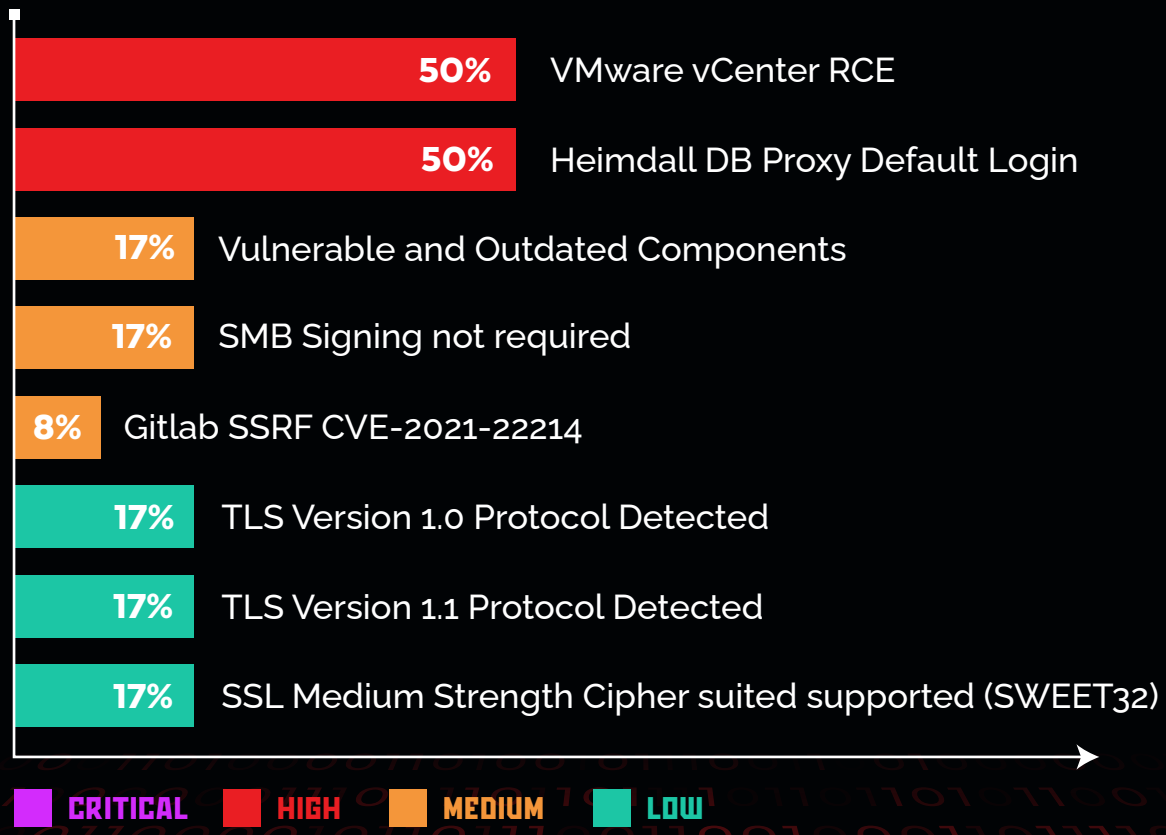
OPERATING SYSTEMS

In this section, we explore the vulnerabilities in detail for operation systems, focusing on virtual machines (VMs), servers, and workstations. Our findings reveal both strengths and areas of concern, with high-risk vulnerabilities posing significant threats to system integrity. For VMs and servers, critical risks such as remote code execution vulnerabilities, unauthorized access, and misconfigurations were identified, alongside medium and low-risk issues that highlight the need for consistent patching, configuration hardening, and access control. Workstations, while also presenting medium to low-risk gaps, require enhanced protection to safeguard sensitive data from evolving threats.

SERVERS

Our assessments did not reveal any critical vulnerabilities, which is a positive sign. However, high-risk issues such as VMware vCenter Remote Code Execution (RCE) and Heimdall DB Proxy default credentials were identified, posing risks of unauthorized access and system compromise.

Medium-risk concerns, including outdated components and an unprotected database dump, highlighted weaknesses in patch management and data security. Additionally, low-risk findings like outdated TLS versions indicated areas needing improvement. Addressing these issues through regular updates, access restrictions, and encryption will help strengthen server defenses.



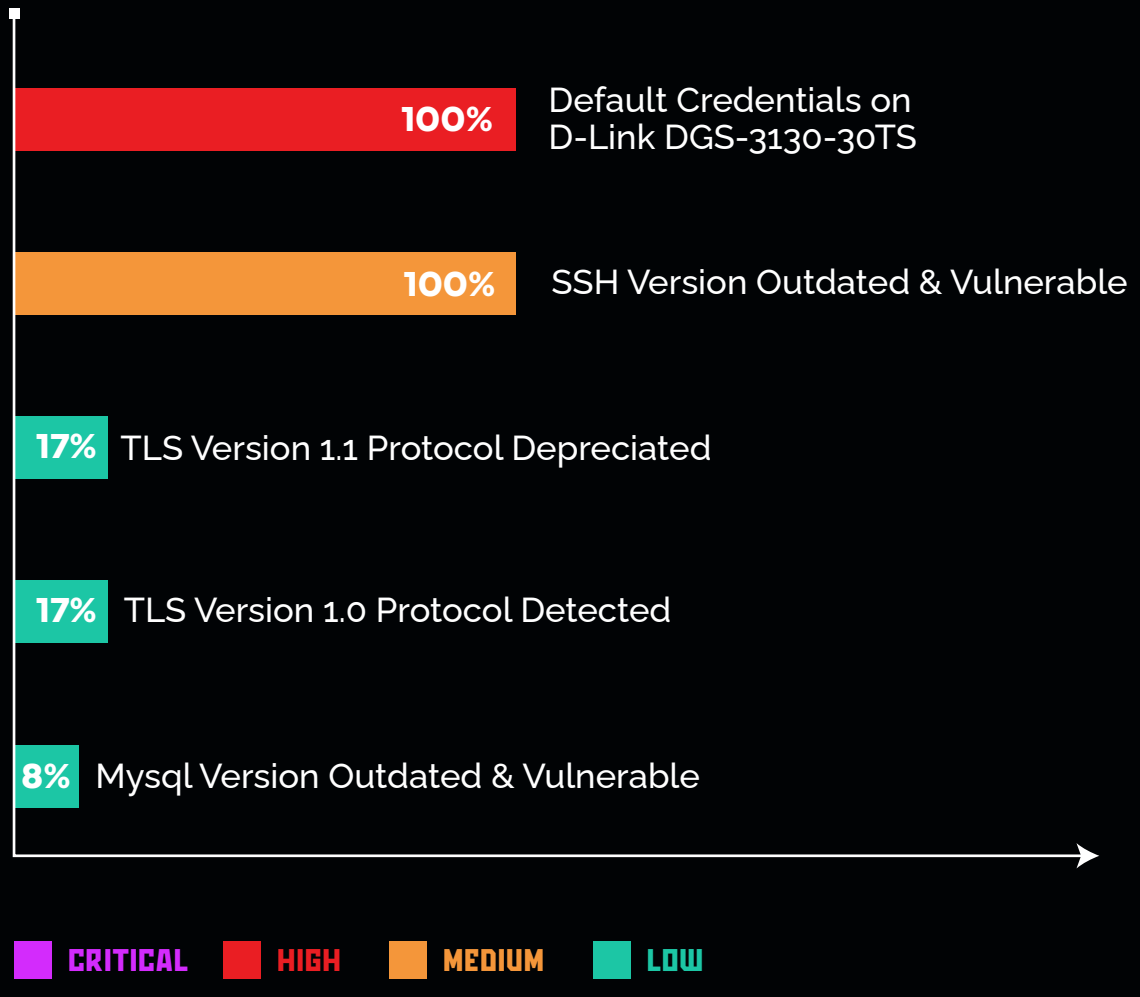
*Disclaimer: The graph displays the top critical & high, medium & low vulnerabilities.

NETWORK DEVICES

Our assessments of network devices, while we did not uncover any critical vulnerabilities, we did identify a high-risk vulnerability related to default credentials on a D-Link DGS-3130-30TS device. While this was the only high-risk finding in network devices, it highlights a significant security concern. Additionally, outdated SSH versions were found, potentially allowing unauthorized access.

Medium-risk findings included deprecated TLS 1.0 and 1.1 protocols (17% each) and outdated MySQL versions (8%), which could expose sensitive data if not addressed. Low-risk concerns, such as outdated encryption protocols, indicate areas where security improvements are needed.

To strengthen network security, organizations should implement regular patching, enforce stricter authentication policies, and upgrade encryption practices to mitigate potential risks.

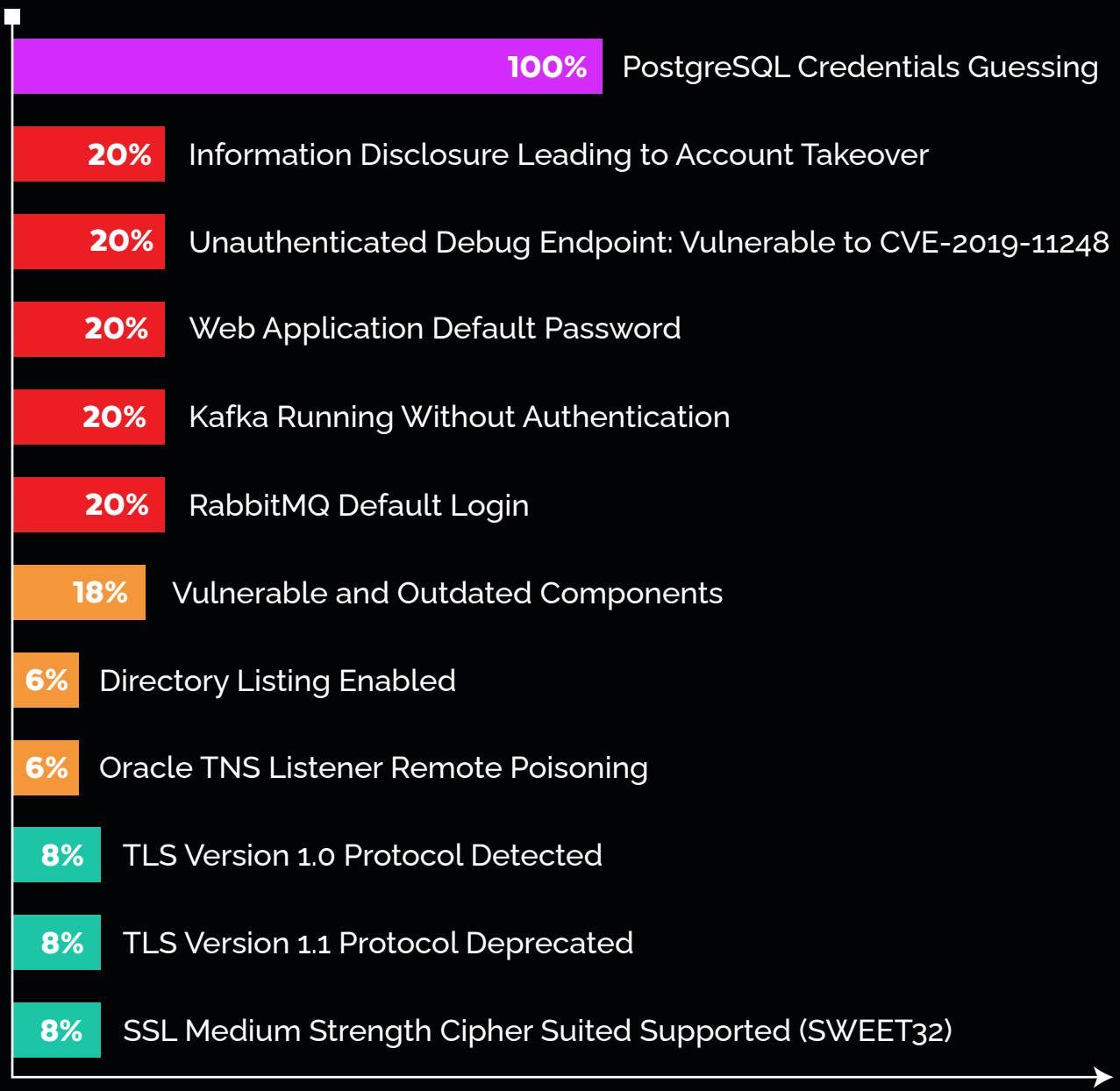


*Disclaimer: The graph displays the top critical & high, medium & low vulnerabilities.

VIRTUAL MACHINES (VMs)

Our assessments of virtual machines (VMs) identified a critical security risk: PostgreSQL credential guessing, which could allow unauthorized access to sensitive systems. Several high-risk vulnerabilities were also uncovered, including information disclosure leading to account takeover, an unauthenticated debug endpoint, default web application passwords, and unsecured Kafka and RabbitMQ instances.

Medium-risk issues—such as outdated components and directory listing being enabled—further increased exposure. Additionally, low-risk concerns like outdated TLS versions and weak SSL ciphers highlight areas where security hardening is needed to reduce potential attack vectors.

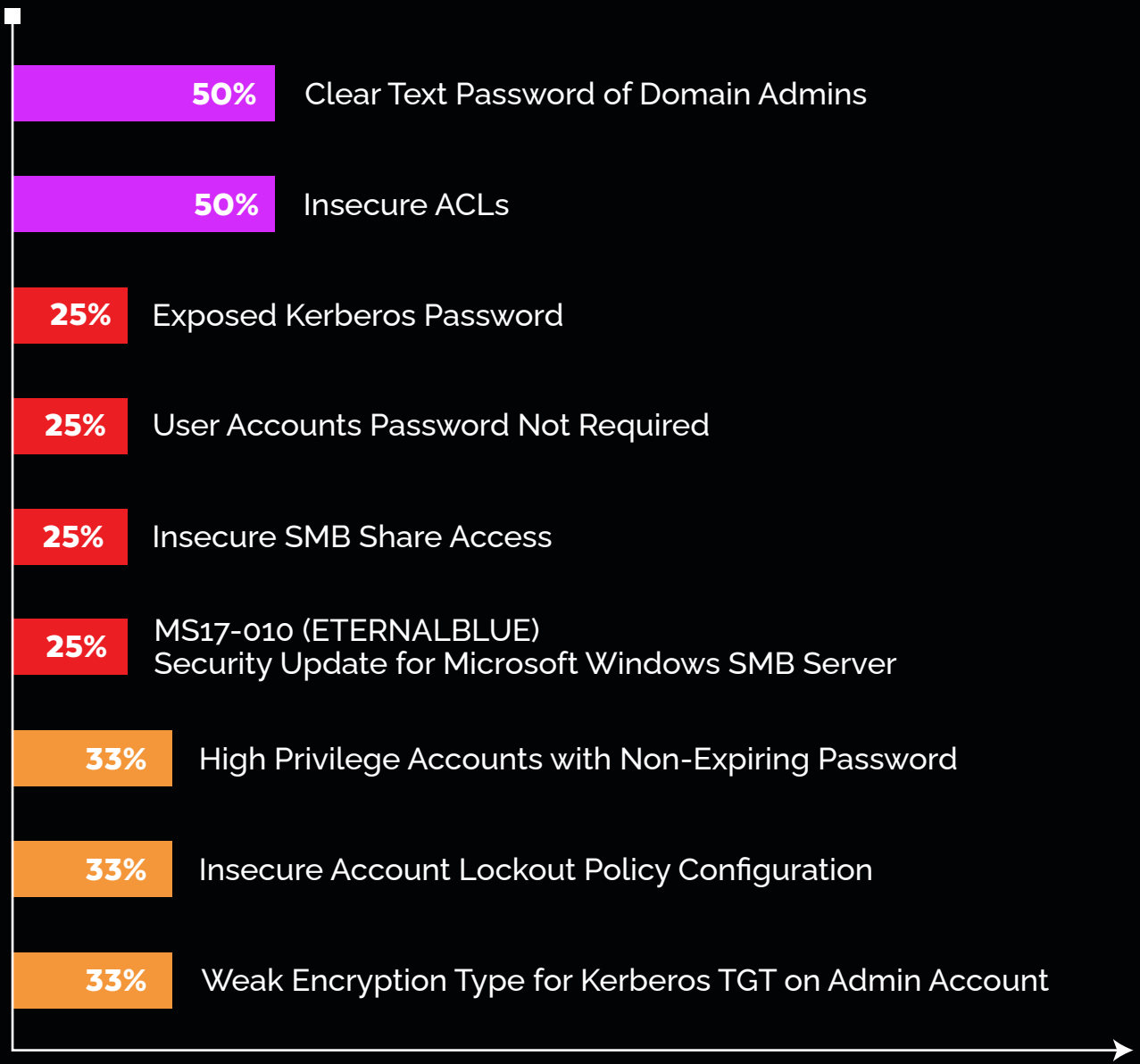


*Disclaimer: The graph displays the top critical & high, medium & low vulnerabilities.

ACTIVE DIRECTORY

Our assessments of Active Directory environments uncovered critical security risks that require immediate attention. Domain admin passwords stored in clear text and insecure ACLs pose significant threats, potentially allowing attackers to escalate privileges.

High-risk vulnerabilities were also prevalent, including exposed Kerberos passwords, user accounts without password requirements, insecure SMB shares, and the presence of the MS17-010 (ETERNALBLUE) exploit. Additionally, medium-risk issues—such as high-privilege accounts with non-expiring passwords, weak Kerberos encryption, and insecure account lockout policies—further weakened defenses. Addressing these gaps is essential to maintaining a secure and resilient Active Directory infrastructure.

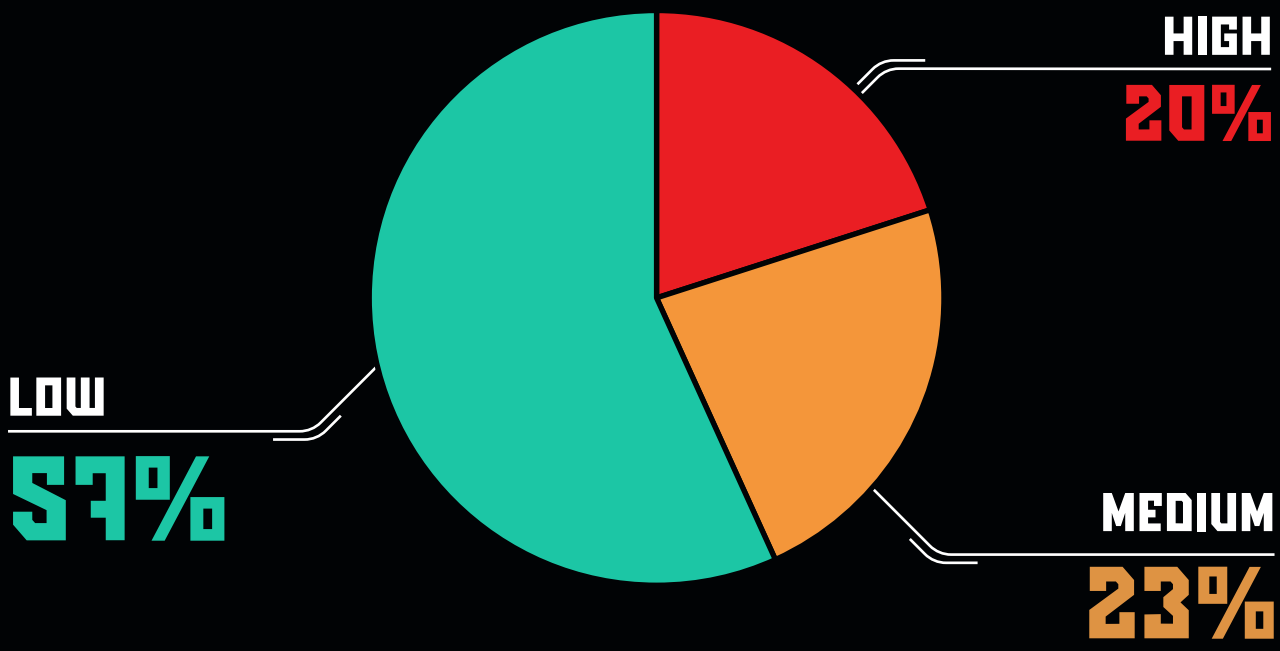


*Disclaimer: The graph displays the top critical & high, medium & low vulnerabilities.

SECTOR-WISE VULNERABILITIES

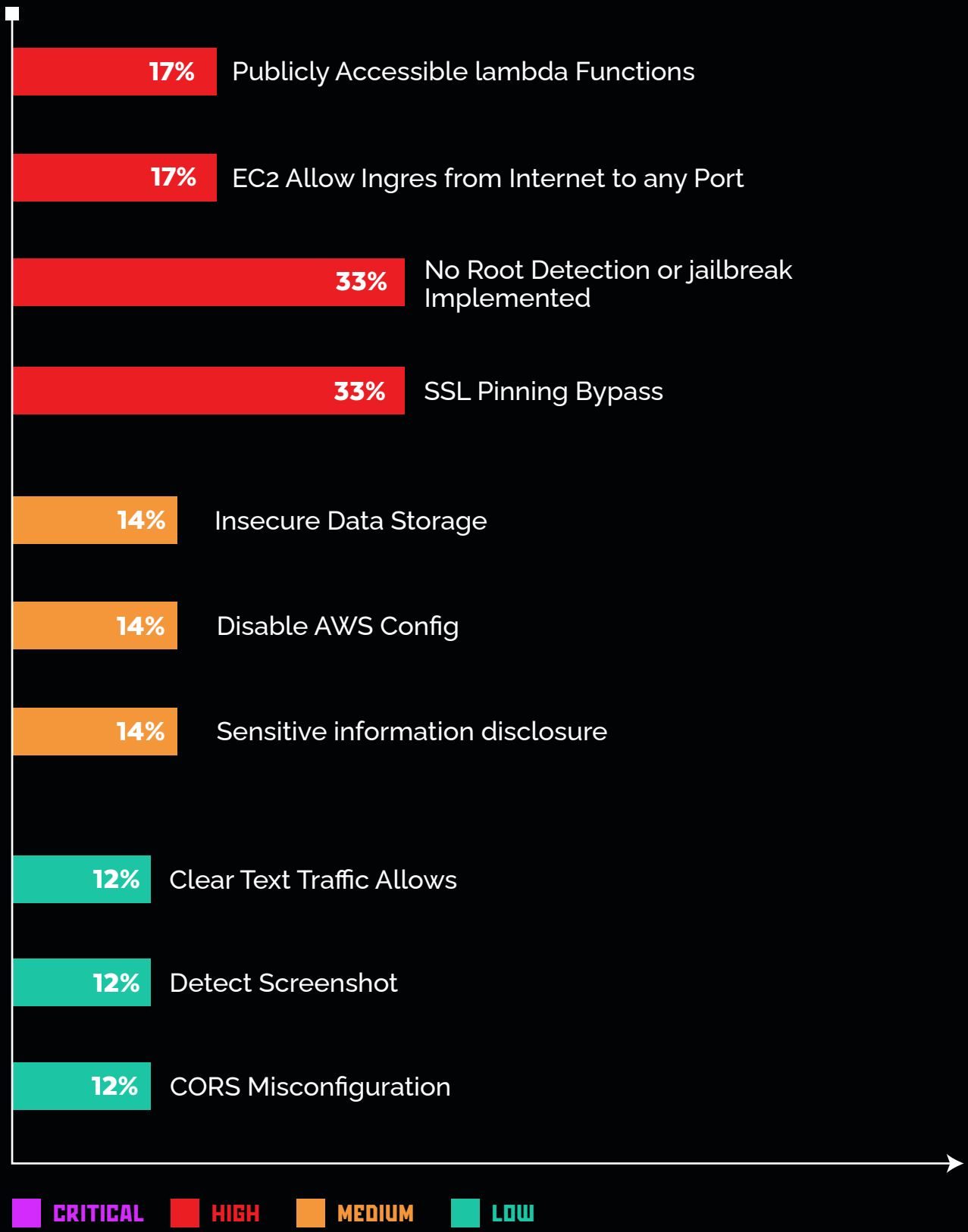
IT & SOFTWARE SECTOR

Modern businesses rely on IT and software companies to develop and maintain the applications, platforms, and infrastructure that power their operations. From cloud service providers and enterprise software firms to SaaS platforms and mobile app developers, these organizations play a crucial role in digital transformation. Their central position in the tech ecosystem makes them prime targets for cyber threats—whether for financial gain, intellectual property theft, or large-scale supply chain attacks. A single vulnerability in widely used software can have a ripple effect, impacting countless businesses and users.



Our assessments revealed no critical vulnerabilities in this sector. High-risk issues, such as publicly accessible Lambda functions and EC2 instances with open ingress ports, expose systems to potential breaches. Medium-risk concerns, including insecure data storage and disabled AWS Config, weaken security controls, while low-risk misconfigurations, such as cleartext traffic and CORS issues, further expand the attack surface. The combination of complex software dependencies, frequent updates, and evolving attack techniques underlines the need for continuous security monitoring, secure coding practices, and robust access controls to protect sensitive data and maintain trust in digital ecosystems.

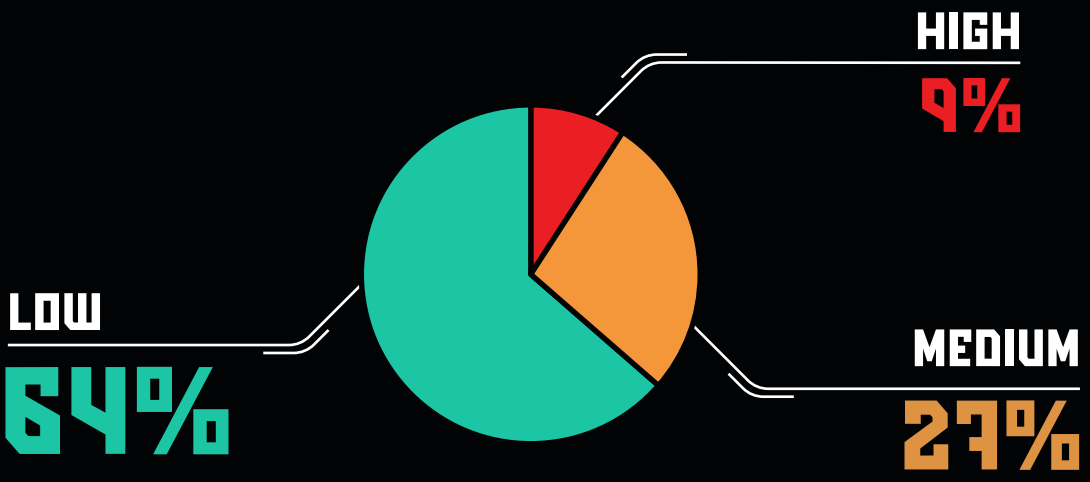
MOST PREVALENT VULNERABILITIES IN IT & SOFTWARE SECTOR



*Disclaimer: The graph displays the top critical & high, medium & low vulnerabilities.

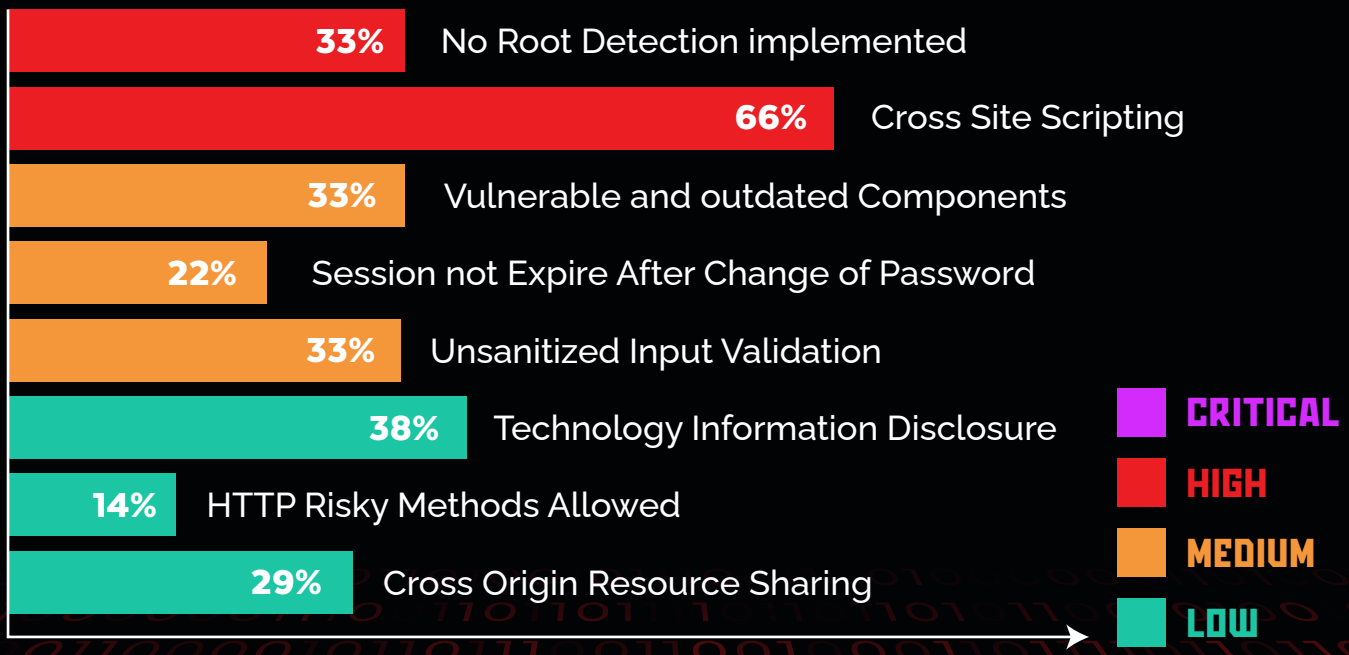
BANKING SECTOR

As the backbone of the global financial system, banks and financial institutions handle vast amounts of transactions and safeguard highly sensitive customer data. Their critical role makes them a prime target for cybercriminals, who seek financial gain or exploit systemic weaknesses for large-scale fraud. With increasing digitalization, the attack surface continues to grow, requiring banks to stay ahead of evolving threats to protect both assets and trust.



Our assessments identified significant security concerns in this sector. While no critical vulnerabilities were found, high-risk issues—such as cross-site scripting and the absence of root detection—pose potential threats to banking applications. Additionally, outdated components, session management flaws, and weak input validation contribute to security gaps, increasing the risk of exploitation. Given the high stakes involved, continuous security improvements, strict access controls, and proactive threat mitigation are essential to maintaining resilience in financial systems.

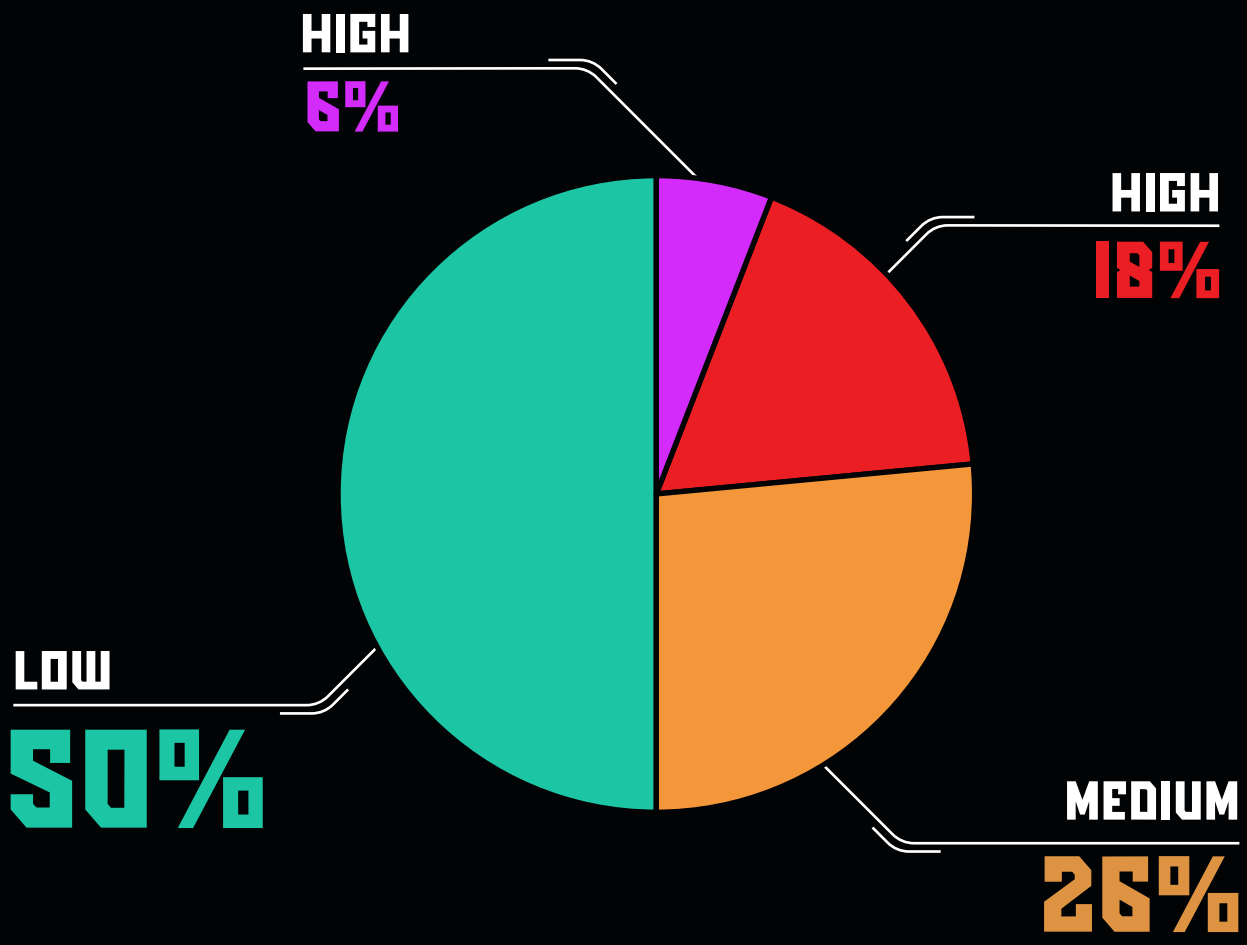
MOST PREVALENT VULNERABILITIES IN BANKING SECTOR



*Disclaimer: The graph displays the top critical & high, medium & low vulnerabilities.

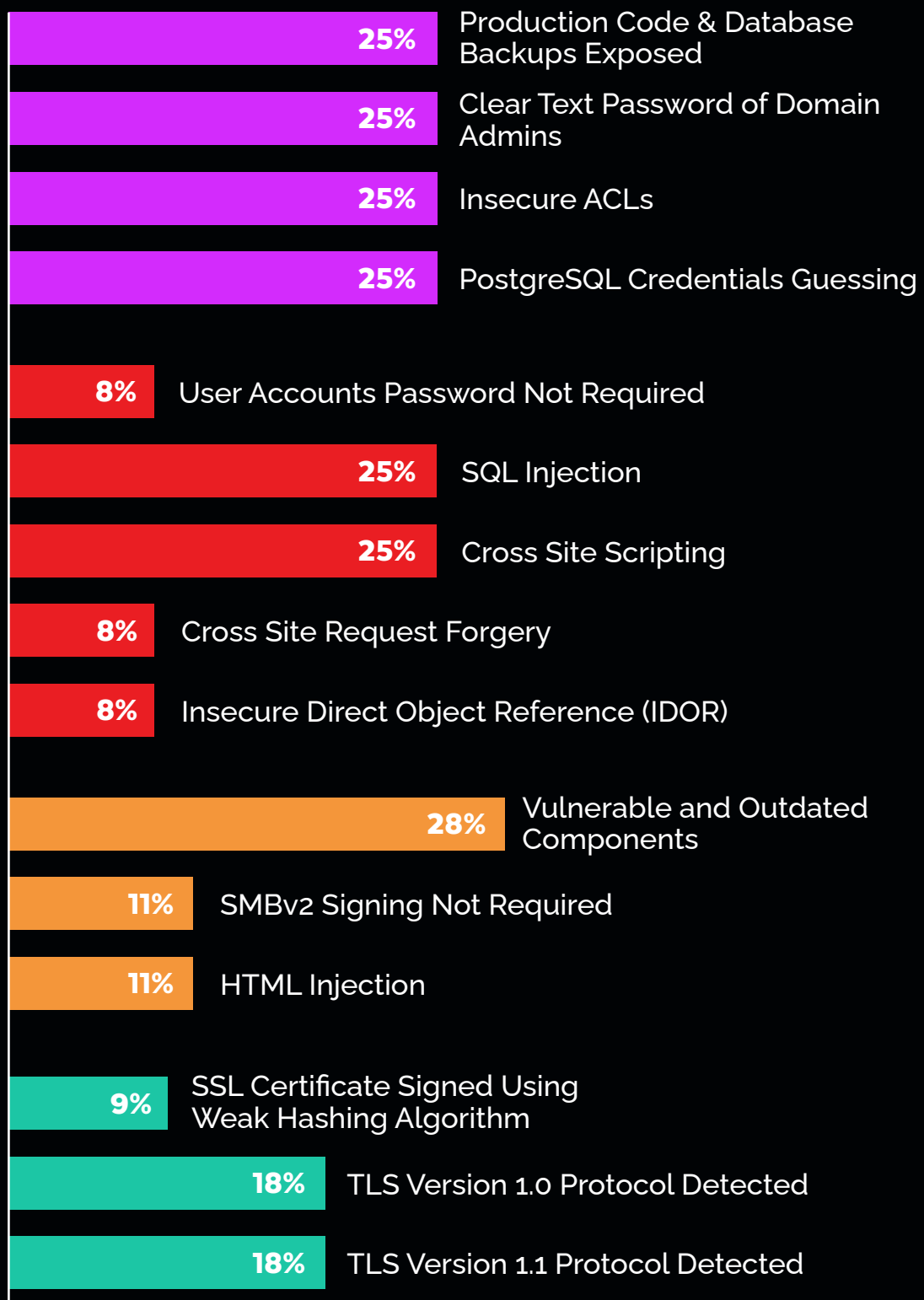
GOVERNMENT SECTOR

Government institutions are responsible for national security, essential public services, and safeguarding vast amounts of citizen data. This makes them a prime target for cyberattacks aimed at disrupting critical infrastructure, stealing sensitive information, or undermining public trust. With an ever-evolving threat landscape, ensuring robust security measures is crucial to protecting these systems from exploitation.



Our assessments revealed significant vulnerabilities in government systems. Critical risks—such as exposed production code, database backups, cleartext domain admin passwords, and insecure ACLs—pose severe threats to data integrity and access control. Additionally, high-risk issues, including SQL injection and cross-site scripting, highlight weaknesses in application security. A considerable number of medium and low-risk vulnerabilities, such as outdated components and insecure configurations, further expand the attack surface. Addressing these gaps through stronger access controls, regular patching, and secure development practices is essential to fortifying the sector against evolving cyber threats.

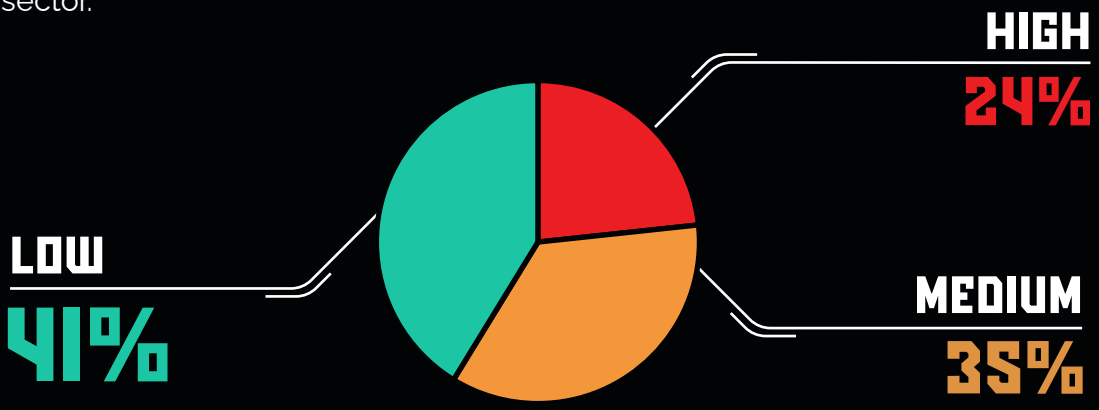
MOST PREVALENT VULNERABILITIES IN GOVERNMENT SECTOR



*Disclaimer: The graph displays the top critical & high, medium & low vulnerabilities.

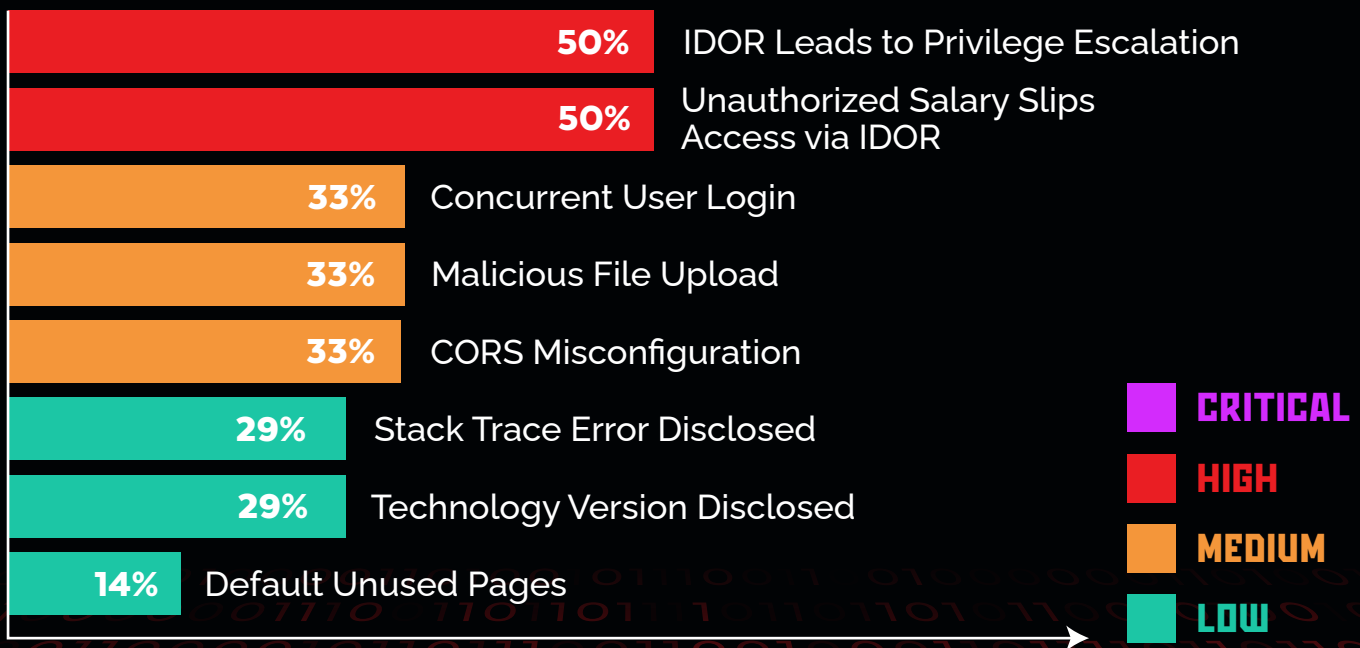
EDUCATION SECTOR

Educational institutions play a vital role in shaping future generations while managing vast amounts of sensitive student and faculty data. From K-12 schools to universities, these institutions store personal records, academic research, and financial information, making them attractive targets for cyberattacks. Limited resources, outdated infrastructure, and a diverse user base with varying security awareness levels further complicate cybersecurity efforts in this sector.



Our assessments identified significant security concerns in education systems. High-risk vulnerabilities, such as Insecure Direct Object References (IDOR), create opportunities for privilege escalation and unauthorized access to sensitive data like salary slips. Additionally, concurrent user login issues and malicious file upload flaws expose weaknesses in access control and input validation. While no critical vulnerabilities were found, the presence of medium and low-risk issues highlights the urgent need for stronger authentication measures, secure coding practices, and regular security assessments to protect both institutional and student data.

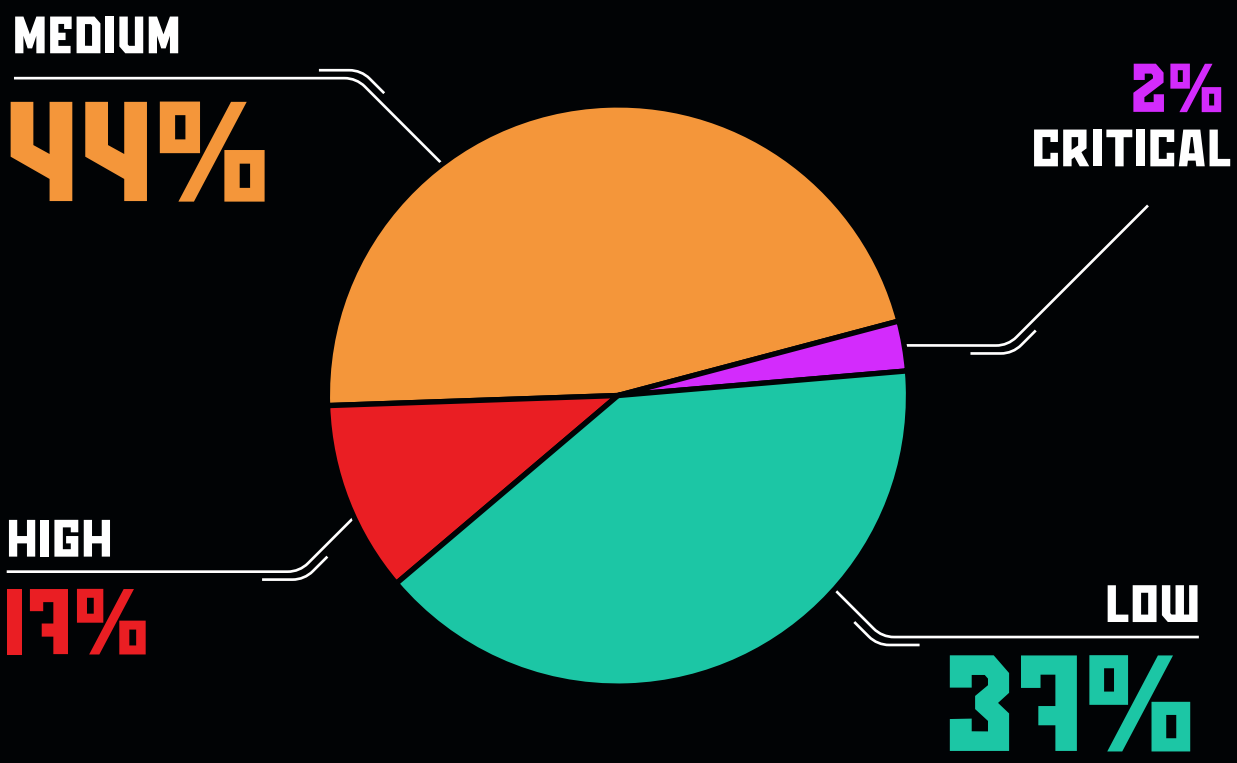
MOST PREVALENT VULNERABILITIES IN EDUCATION SECTOR



*Disclaimer: The graph displays the top critical & high, medium & low vulnerabilities.

MANUFACTURING SECTOR

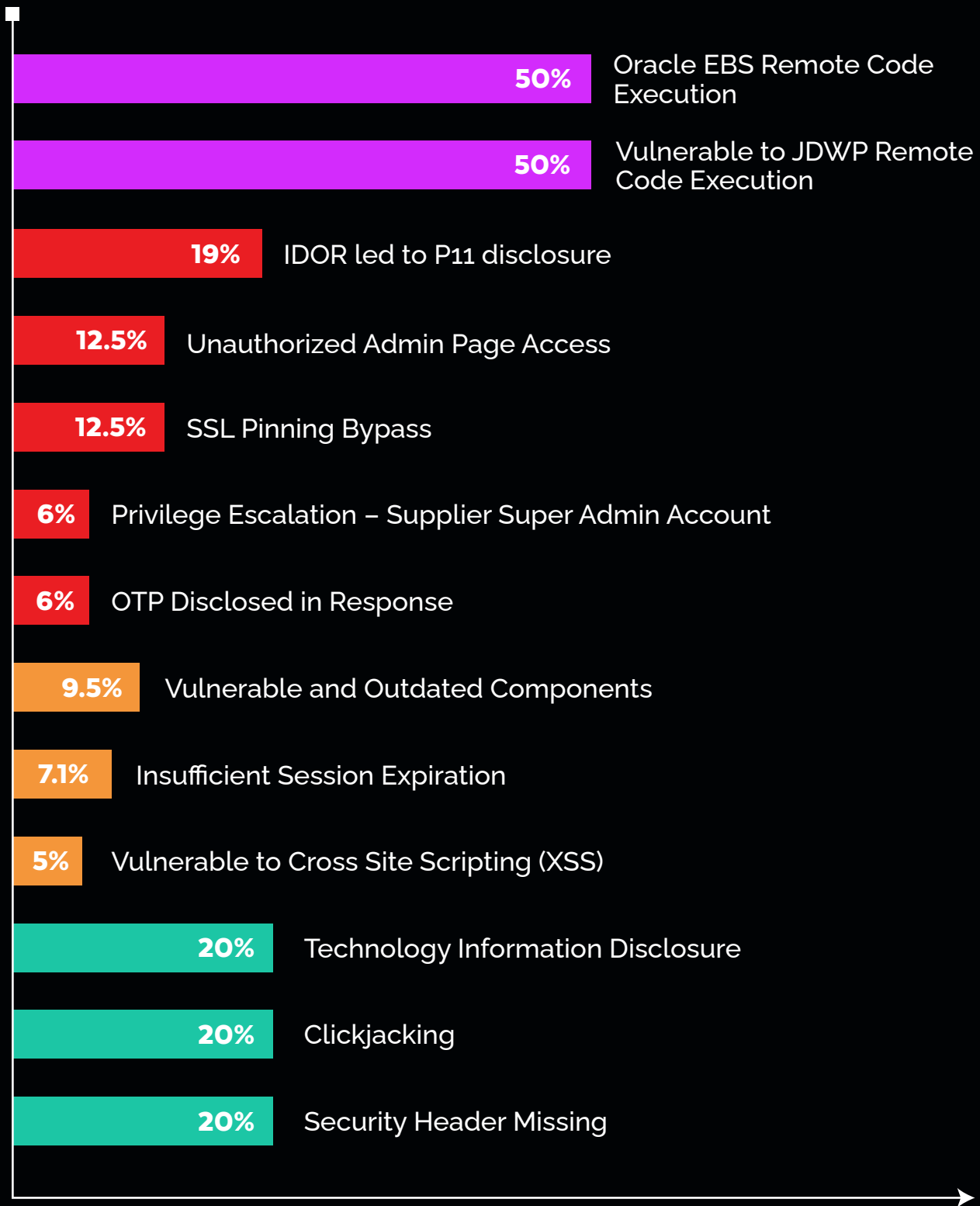
The manufacturing sector, a cornerstone of industrial production and global trade, faces growing cybersecurity challenges as it undergoes digital transformation. From automated production lines to supply chain management systems, interconnected networks enhance efficiency but also expand the attack surface. Manufacturers must safeguard proprietary designs, operational technology, and sensitive business data—making them prime targets for cyberattacks. Disruptions can result in financial losses, production halts, and compromised intellectual property.



Our assessments reveal a concerning security landscape. 17% of identified vulnerabilities were high-risk, with threats such as unauthorized admin access, privilege escalation, and insecure authentication mechanisms exposing critical systems. Additionally, 2% of vulnerabilities were classified as critical, including remote code execution flaws in Oracle EBS and JDWP, SSL pinning bypass, and information disclosure leading to account takeovers. 44% of vulnerabilities fell under the medium-risk category, while 37% were classified as low-risk, highlighting issues like missing security headers and HTML injection that further emphasize the need for stronger security controls.

As manufacturing continues to embrace automation and digital integration, implementing stringent access controls, secure authentication protocols, and continuous security monitoring is essential to protect against evolving cyber threats.

MOST PREVALENT VULNERABILITIES IN MANUFACTURING SECTOR

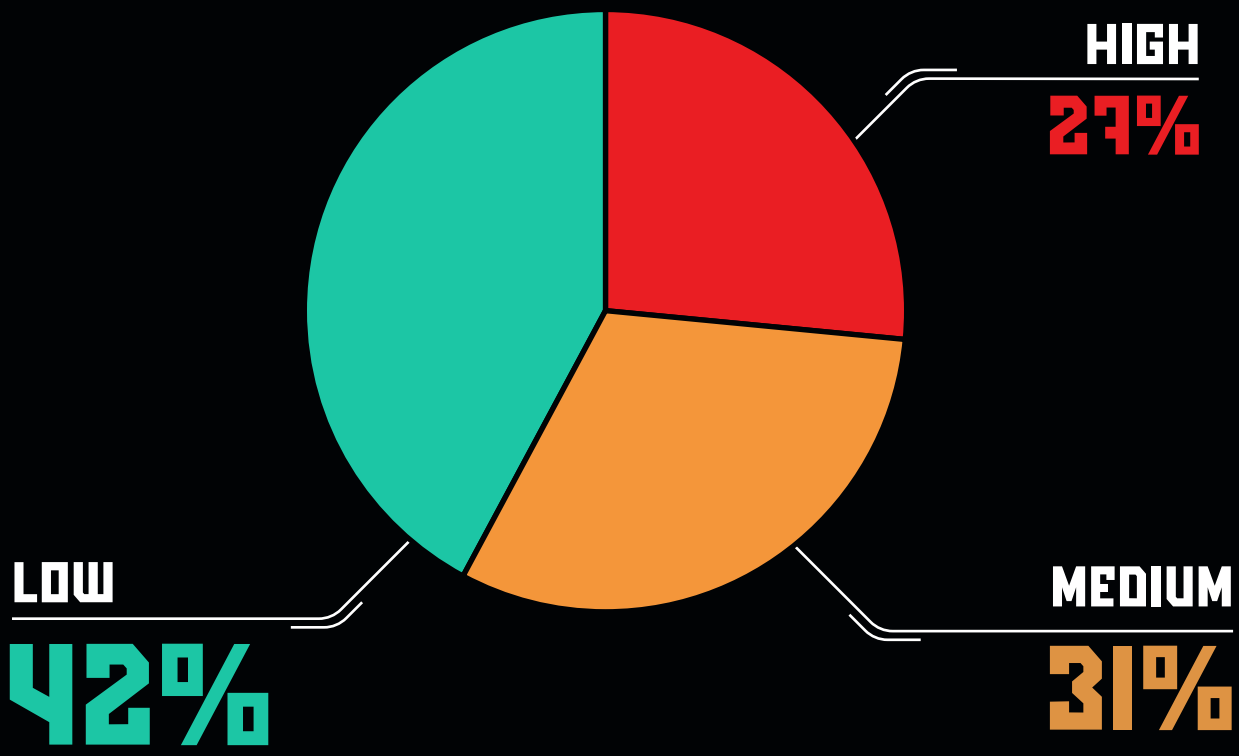


CRITICAL HIGH MEDIUM LOW

*Disclaimer: The graph displays the top critical & high, medium & low vulnerabilities.

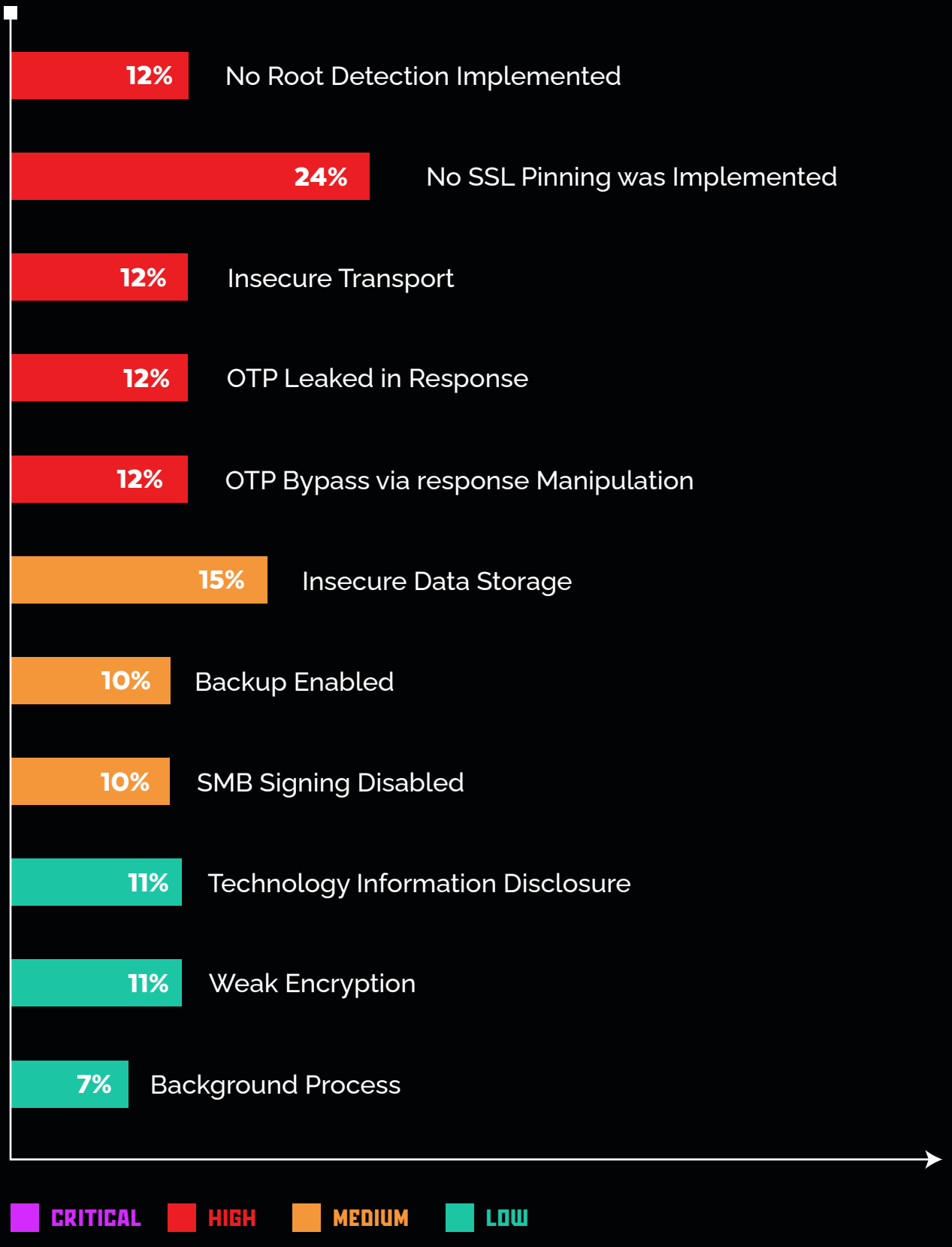
HEALTHCARE SECTOR

The healthcare sector, a critical pillar of society, is responsible for protecting sensitive patient data and ensuring the uninterrupted delivery of essential medical services. As hospitals and healthcare providers increasingly adopt digital solutions—ranging from electronic health records (EHRs) and telehealth platforms to connected medical devices—their cybersecurity risks grow exponentially. This sector is a prime target for cybercriminals due to the vast amounts of protected health information (PHI) it manages, making it vulnerable to ransomware attacks, data breaches, and disruptions that could impact patient care. The complexity of interconnected systems across medical, administrative, and research networks further expands the attack surface, requiring a proactive approach to security.



Our assessment reveals that the healthcare sector faces significant cybersecurity risks, with 42% of vulnerabilities classified as high-risk. Key concerns include the lack of SSL pinning, exposing sensitive patient data to potential interception, as well as stored cross-site scripting and insecure transport mechanisms that undermine application security. Additionally, weaknesses in access controls and outdated software components further increase exposure to cyber threats. Strengthening security measures through robust encryption, network segmentation, and regular vulnerability assessments is essential to safeguarding patient data and ensuring the resilience of healthcare infrastructure.

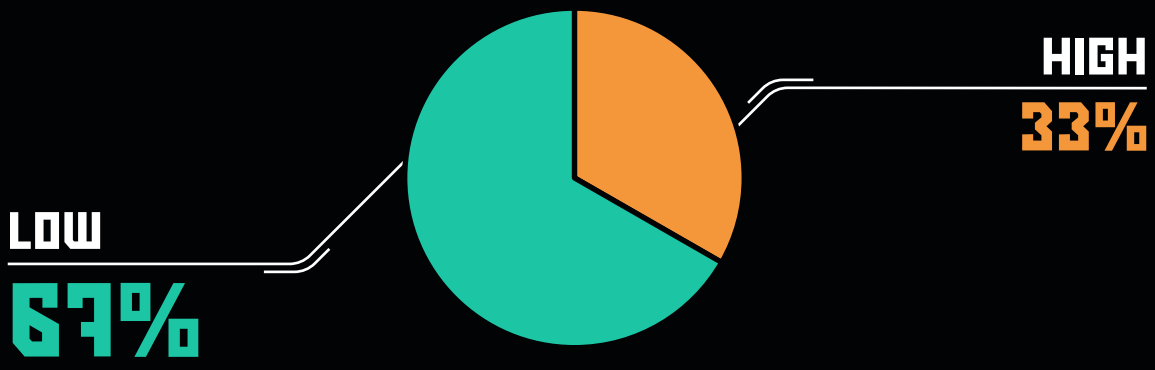
MOST PREVALENT VULNERABILITIES IN HEALTHCARE SECTOR



*Disclaimer: The graph displays the top critical & high, medium & low vulnerabilities.

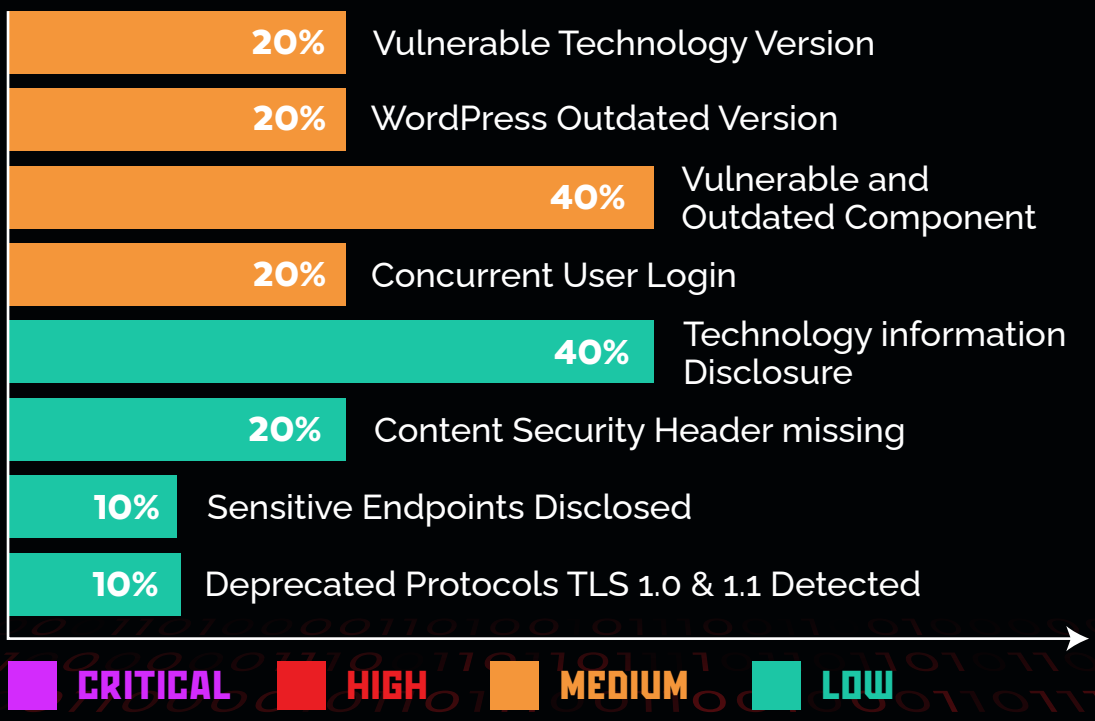
TELECOMMUNICATION SECTOR

The telecommunications sector serves as the foundation of modern communication, enabling global connectivity through voice, data, and internet services. As telecom networks become increasingly software-driven and reliant on cloud technologies, they also face a growing array of cyber threats. With vast amounts of sensitive user data—such as call records, location information, and personal details—this sector remains a prime target for cybercriminals seeking financial gain, espionage, or service disruption. Attacks on telecom infrastructure can have far-reaching consequences, affecting businesses, governments, and individuals alike.



Our assessment highlights a range of vulnerabilities, primarily in the medium and low-risk categories. Outdated software versions, including WordPress and other critical components, create entry points for attackers, while concurrent user login vulnerabilities pose security risks related to unauthorized access. These findings emphasize the need for regular patch management, stringent access controls & robust network monitoring.

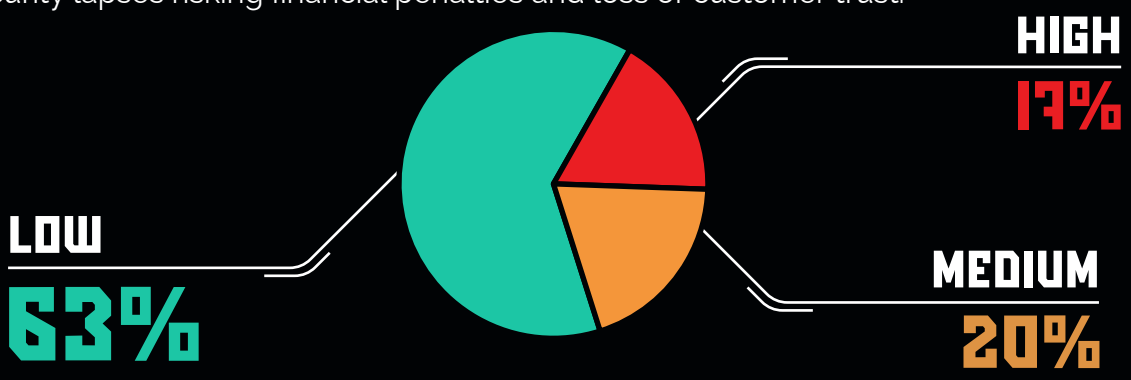
MOST PREVALENT VULNERABILITIES IN TELECOMMUNICATION SECTOR



*Disclaimer: The graph displays the top critical & high, medium & low vulnerabilities.

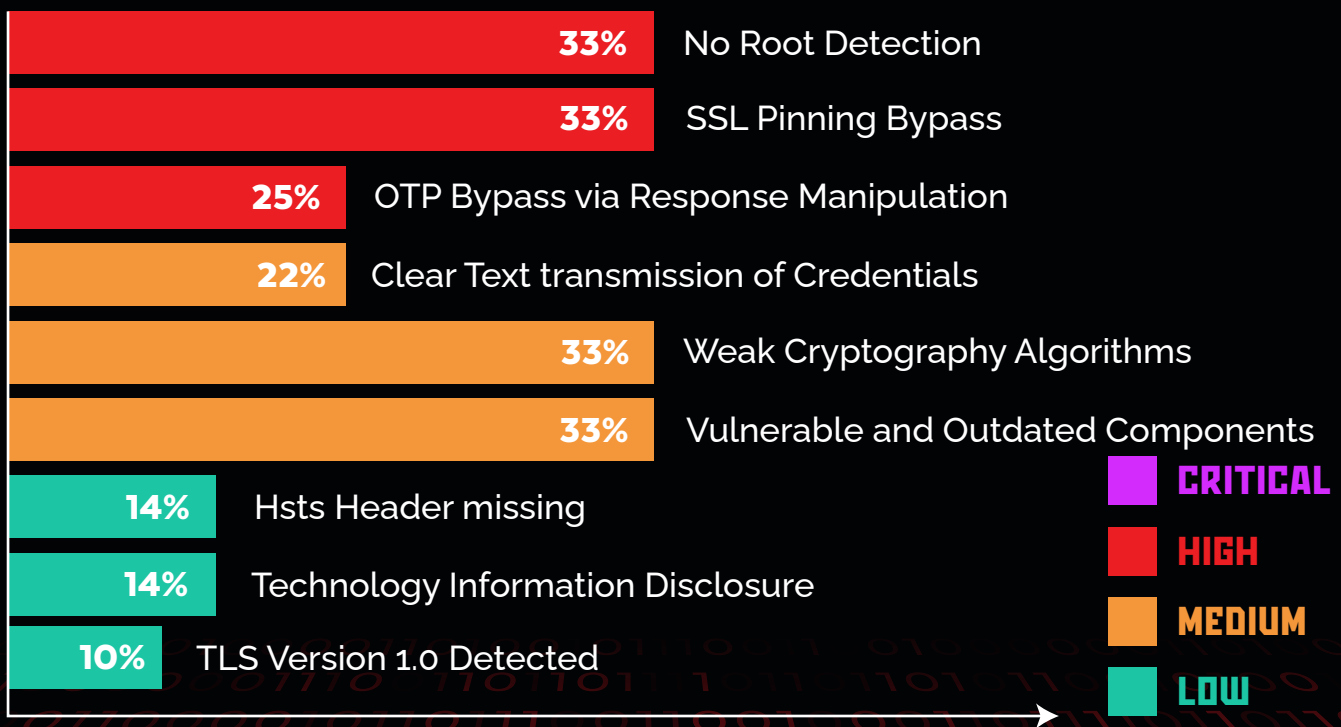
FINTECH SECTOR

The fintech sector, driving digital financial services through mobile banking, payment gateways, lending and investment platforms, faces persistent cyber threats due to its reliance on cloud infrastructure, open banking APIs, and third-party integrations. Handling vast amounts of sensitive user data, the fintech sector remains a prime target for cybercriminals exploiting weak API security, outdated encryption methods, and unprotected mobile applications. The evolving regulatory landscape in fintech makes compliance with data protection laws (e.g., GDPR, PCI-DSS) an ongoing challenge. Rapid digital finance adoption adds pressure, with security lapses risking financial penalties and loss of customer trust.



Our assessments revealed high-severity vulnerabilities such as SSL Pinning Bypass & No Root Detection, exposing fintech applications to data interception and reverse engineering. Additionally, weak cryptographic algorithms and cleartext credential transmission highlight encryption flaws that could compromise sensitive transactions. Addressing these gaps requires fintech firms to strengthen API security, implement robust encryption standards, and enforce strict access controls to mitigate the risk of data breaches and financial fraud.

MOST PREVALENT VULNERABILITIES IN FINTECH SECTOR



*Disclaimer: The graph displays the top critical & high, medium & low vulnerabilities.

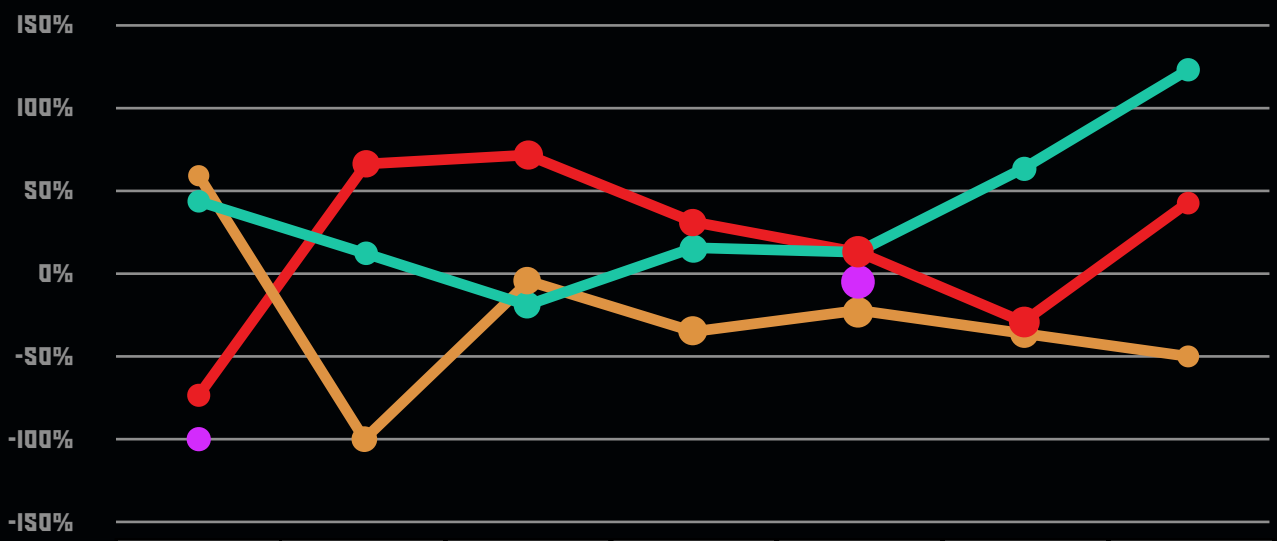
VULNERABILITY TRENDS

YEAR-OVER-YEAR ANALYSIS (2023-2024)

SECTOR	CATEGORY	2023 (%)	2024 (%)	% CHANGE
BANKING	CRITICAL	4.6		-100%
	HIGH	33.6	9	-73%
	MEDIUM	17.1	27	58%
	LOW	44.5	64	44%
TELECOM	CRITICAL			
	HIGH	20	33	65%
	MEDIUM	20		-100%
	LOW	60	67	12%
EDUCATION	CRITICAL			
	HIGH	14	24	71%
	MEDIUM	43	41	-5%
	LOW	43	35	-19%
IT & SOFTWARE	CRITICAL			
	HIGH	15.4	20	30%
	MEDIUM	35.4	23	-35%
	LOW	49.2	57	16%
GOVERNMENT	CRITICAL	6.4	6	-6%
	HIGH	16.1	18	12%
	MEDIUM	33.5	26	-22%
	LOW	44	50	14%
MANUFACTURING	CRITICAL			
	HIGH	16.9	12	-29%
	MEDIUM	48.2	31	-36%
	LOW	34.9	57	63%
HEALTHCARE	CRITICAL			
	HIGH	18.88	27	43%
	MEDIUM	17.1	31	81%
	LOW	18.88	42	122%

*Disclaimer: In the % Change column, Green indicates decline in vulnerabilities leading to improved security, and red signals a rise in vulnerabilities since last year, pointing to worsened security.

YEAR-OVER-YEAR COMPARISON (2023 VS 2024)



	BANKING	TELECOM	EDUCATION	IT & SOFTWARE	GOVERNMENT	MANUFACTURING	HEALTHCARE
HIGH	-73%	65%	71%	30%	12%	-29%	43%
MEDIUM	58%	-100%	-5%	-35%	-22%	-36%	-51%
LOW	44%	12%	-19%	16%	14%	63%	122%
CRITICAL	-100%	N/A	N/A	N/A	-6%	N/A	N/A

The data reveals significant shifts in cybersecurity vulnerabilities across various sectors from 2023 to 2024, with some sectors making significant progress while others face growing threats. The banking sector saw a 100% drop in critical threats and a 73% decline in high-risk issues, reflecting stronger security measures. However, medium (+58%) and low-risk (+44%) vulnerabilities increased, suggesting attackers are still finding smaller gaps to exploit. Telecom experienced a 65% rise in high-risk vulnerabilities, while medium-risk threats were eliminated. Education followed a similar trend, with a 71% jump in high-risk vulnerabilities, highlighting its increasing exposure to cyber threats.

The IT & Software and government sectors had mixed results. The IT sector's high-risk vulnerabilities rose by 30%, while medium-risk threats dropped sharply, possibly indicating shifting attack strategies. The government sector remained stable, with only minor fluctuations. In manufacturing, high and medium vulnerabilities declined, but low-risk vulnerabilities surged by 63%, pointing to emerging risks. Healthcare saw the most dramatic changes, with high-risk vulnerabilities up 43% and low-risk vulnerabilities soaring 122%, suggesting attackers are probing for weaknesses before launching more severe attacks. These changes highlight the evolving threat landscape and the need for businesses to continuously adapt their security strategies.

CONCLUSION

This report offers a data-driven analysis of Pakistan's cybersecurity landscape, highlighting critical vulnerabilities uncovered through the 2024 penetration testing conducted by Trillium Information Security Systems (TISS). Our findings reveal that sectors such as banking, pharmaceuticals, education, and government face systemic security challenges, often due to outdated systems, misconfigurations, and weak access controls. These gaps not only expose sensitive data to cyber threats but also undermine the resilience of digital infrastructures.

A key takeaway from our research is the recurring pattern of vulnerabilities across industries—ranging from weak authentication and insecure data storage to insufficient patch management. This suggests that many organizations still prioritize functionality over security, leaving them susceptible to exploitation.

Addressing these risks requires a shift in mindset: cybersecurity must be integrated into the foundation of business operations rather than treated as an afterthought. Proactive measures such as regular penetration testing, secure software development practices, and robust employee training can significantly reduce attack surfaces and enhance overall security posture.

Beyond identifying risks, this report serves as a strategic guide for organizations looking to fortify their defenses. By leveraging these insights, businesses can implement targeted improvements, mitigate emerging threats, and build more resilient cybersecurity frameworks.

At TISS, we are committed to empowering security teams, developers, and decision-makers with the knowledge they need to stay ahead of evolving cyber threats—creating a safer and more secure digital ecosystem for all.

MOST COMMONLY DETECTED THREATS

TECHNOLOGY INFORMATION DISCLOSURE

OCCURRENCES: 33

SECTORS AFFECTED: IT & Software, Banking, Education, Manufacturing, Healthcare, Telecom, FinTech

VULNERABLE AND OUTDATED COMPONENTS

OCCURRENCES: 27

SECTORS AFFECTED: Banking, Government, Manufacturing, FinTech, Telecom

SSL PINNING BYPASSED

OCCURRENCES: 13

SECTORS AFFECTED: IT & Software, FinTech & Manufacturing

TLS VER 1.0 & 1.1 PROTOCOLS DETECTED

OCCURRENCES: 16

SECTORS AFFECTED: Telecom, Government, FinTech